

Servidores proxy e tunelamento

Ao navegar por diferentes redes da Internet, servidores proxy e túneis HTTP facilitam o acesso ao conteúdo na World Wide Web.

Um proxy pode estar no computador local do usuário, ou em qualquer lugar entre o computador do usuário e um servidor de destino na Internet.

Esta página apresenta alguns conceitos básicos sobre proxies e introduz algumas opções de configuração.

Existem dois tipos de proxies: **proxies de encaminhamento** (ou túnel, ou gateway) e **proxies reversos** (usados para controlar e proteger o acesso a um servidor para balanceamento de carga, autenticação,criptografia ou cache).

Proxies de encaminhamento

Um **proxy de encaminhamento**, ou gateway, ou simplesmente "proxy", fornece serviços de proxy para um cliente ou grupo de clientes.

Provavelmente existem centenas de milhares de proxies de encaminhamento abertos na Internet.

Eles armazenam e encaminham serviços da Internet (como DNS ou páginas web) para reduzir e controlar a largura de banda usada pelo grupo.

Proxies de encaminhamento também podem ser **anônimos** e permitir que os usuários ocultem seu endereço IP ao navegar na Web ou usar outros serviços da Internet.

Por exemplo, o **Tor** encaminha o tráfego da Internet através de múltiplos proxies para garantir anonimato.

Proxies reversos

Como o nome sugere, um **proxy reverso** faz o oposto do que um proxy de encaminhamento faz: um proxy de encaminhamento atua em nome dos clientes (ou hosts solicitantes).

Proxies de encaminhamento podem ocultar a identidade dos clientes, enquanto proxies reversos podem ocultar a identidade dos servidores.

Proxies reversos têm vários casos de uso. Alguns deles são:

- **Balanceamento de carga:** distribuir a carga entre vários servidores web,
 - **Cache de conteúdo estático:** aliviar os servidores web armazenando em cache conteúdo estático como imagens,
 - **Compressão:** comprimir e otimizar conteúdo para acelerar o tempo de carregamento.
-

Encaminhamento de informações do cliente por meio de proxies

Proxies podem fazer com que as requisições pareçam originar-se do endereço IP do próprio proxy.

Isso pode ser útil se um proxy for usado para fornecer anonimato ao cliente, mas em outros casos, informações da requisição original são perdidas.

O endereço IP do cliente original é frequentemente usado para depuração, estatísticas ou geração de conteúdo baseado em localização.

Uma maneira comum de divulgar essas informações é usando os seguintes cabeçalhos HTTP:

O cabeçalho padronizado:

Forwarded

Contém informações do lado voltado para o cliente dos servidores proxy que são alteradas ou perdidas quando um proxy está envolvido no caminho da requisição.

Ou as versões de facto padrão:

- **X-Forwarded-For**
Identifica os endereços IP de origem de um cliente que se conecta a um servidor web através de um proxy HTTP ou um balanceador de carga.
- **X-Forwarded-Host**
Identifica o host original requisitado que um cliente usou para se conectar ao seu proxy ou balanceador de carga.
- **X-Forwarded-Proto**
Identifica o protocolo (HTTP ou HTTPS) que um cliente usou para se conectar ao seu proxy ou balanceador de carga.

Para fornecer informações sobre o próprio proxy (e não sobre o cliente que se conecta a ele), o cabeçalho **Via** pode ser usado.

- **Via**
Adicionado por proxies, tanto de encaminhamento quanto reversos, e pode aparecer nos cabeçalhos de requisição e de resposta.

Tunelamento HTTP

O **tunelamento** transmite dados de redes privadas e informações de protocolos por redes públicas encapsulando os dados.

O **tunelamento HTTP** utiliza um protocolo de nível superior (HTTP) para transportar um protocolo de nível inferior (TCP).

O protocolo HTTP especifica um método de requisição chamado **CONNECT**.

Ele inicia uma comunicação bidirecional com o recurso requisitado e pode ser usado para abrir um túnel.

É assim que um cliente por trás de um proxy HTTP pode acessar sites usando TLS (ou seja, HTTPS, porta 443).

Observe, no entanto, que **nem todos os servidores proxy suportam o método CONNECT**, ou podem **limitá-lo apenas à porta 443**.

Veja também o artigo sobre túnel HTTP na Wikipedia.

Arquivo de Configuração Automática de Proxy (PAC)

Um arquivo **PAC (Proxy Auto-Configuration)** é uma função JavaScript que determina se requisições do navegador web (HTTP, HTTPS e FTP) vão diretamente para o destino ou são encaminhadas para um servidor proxy web.

A função JavaScript contida no arquivo PAC define a função:

O arquivo de configuração automática deve ser salvo com a extensão **.pac** no nome do arquivo:
proxy.pac



E o tipo MIME definido como:

application/x-ns-proxy-autoconfig

O arquivo consiste em uma função chamada FindProxyForURL.

O exemplo abaixo funcionará em um ambiente onde o servidor DNS interno está configurado de modo que **só pode resolver nomes de host internos**, e o objetivo é usar um proxy **apenas para hosts que não são resolvíveis**:

javascript

 Copiar  Editar

```
function FindProxyForURL(url, host) {  
  if (isResolvable(host)) {  
    return "DIRECT";  
  }  
  return "PROXY proxy.mydomain.com:8080";  
}
```